Electronic Version

Stylesheet Version v1.1.1

Claims

[c1] A biometric reader activated by holding the thumb on the reader and plugging into a USB port. This data would be compared to data stored in the solid state memory not the computer, the computer merely recognizes the drive once verification of the fingerprint ID is complete. Once that is complete the computer is restricted to use only the resources designated from the input of the solid state data.

[c2] This device (The Verifier) acts as a physical and elec-tronic key, a place where strong encrypted passwords can be generated and stored without the user having to remember them.

[c3] This device precludes the possibility of someone using a found key. Without the initial thumbprint no data can be accessed.
The software can be programmed to overwrite all data on The Verifier if access is attempted by an inappropriate bio-scan.

[c4] Additional storage area on the solid state memory can be used for sensitive data that is encrypted along with all

the other data on the solid state memory.